

Fig. 1

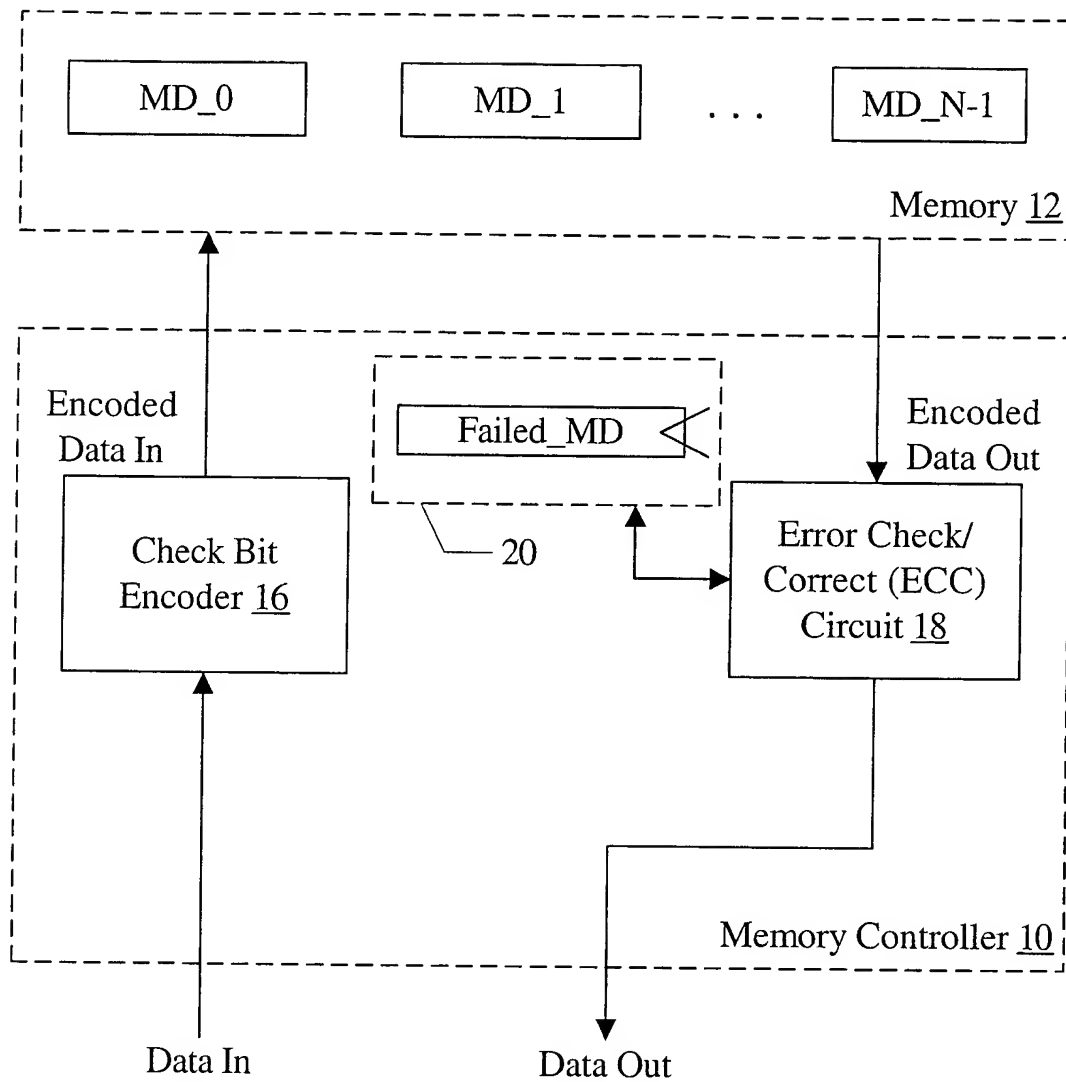


Fig. 2

	c_0	c_1	\dots		c_{N-1}
r_0					
r_1					
	M	M			M
	D	D			D
\vdots			\dots		
\vdots	$\overline{0}$	$\overline{1}$			$\overline{N-1}$
r_{R-1}					

Fig. 3

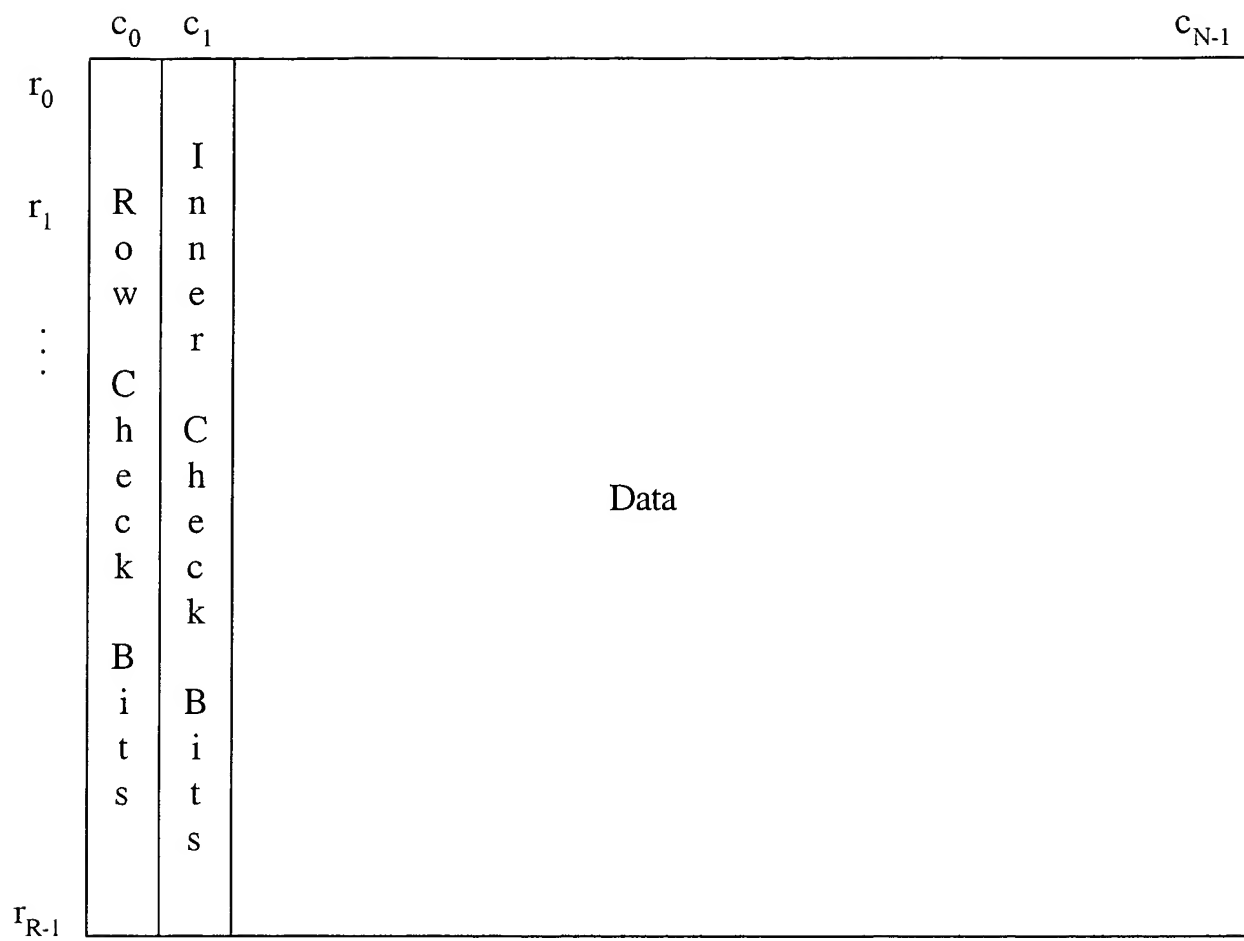


Fig. 4

$$\text{Check_Vector}(r_x, c_y) = \text{key_y} * \alpha^x \quad (\text{in } \text{GF}(2^R)) \quad \longleftarrow 30$$

$$\text{row_syn} * \text{key_i} = \text{inner_syn} \quad (\text{in } \text{GF}(2^R)) \quad \longleftarrow 32$$

$$\begin{aligned} &\text{Check_Vector}(r_1, c_1) \text{ XOR } \text{Check_Vector}(r_2, c_2) \text{ XOR} \\ &\quad \text{Check_Vector}(r_1, c_3) \text{ XOR } \text{Check_Vector}(r_2, c_3) \neq 0 \quad \longleftarrow 34 \\ &\text{for any } r_1, r_2, c_1, c_2, c_3 \text{ such that } ((r_1, c_1) \neq (r_2, c_2) \text{ and } c_1 \neq \\ &\quad c_3) \text{ or } (c_1 \neq c_2) \end{aligned}$$

$$\text{key_i} + \text{key_j} \neq (\text{key_i} + \text{key_k}) * \alpha^X \quad 0 \leq X \leq R-1, i \neq k, i \neq j, j \neq k \quad \longleftarrow 36$$

Fig. 5

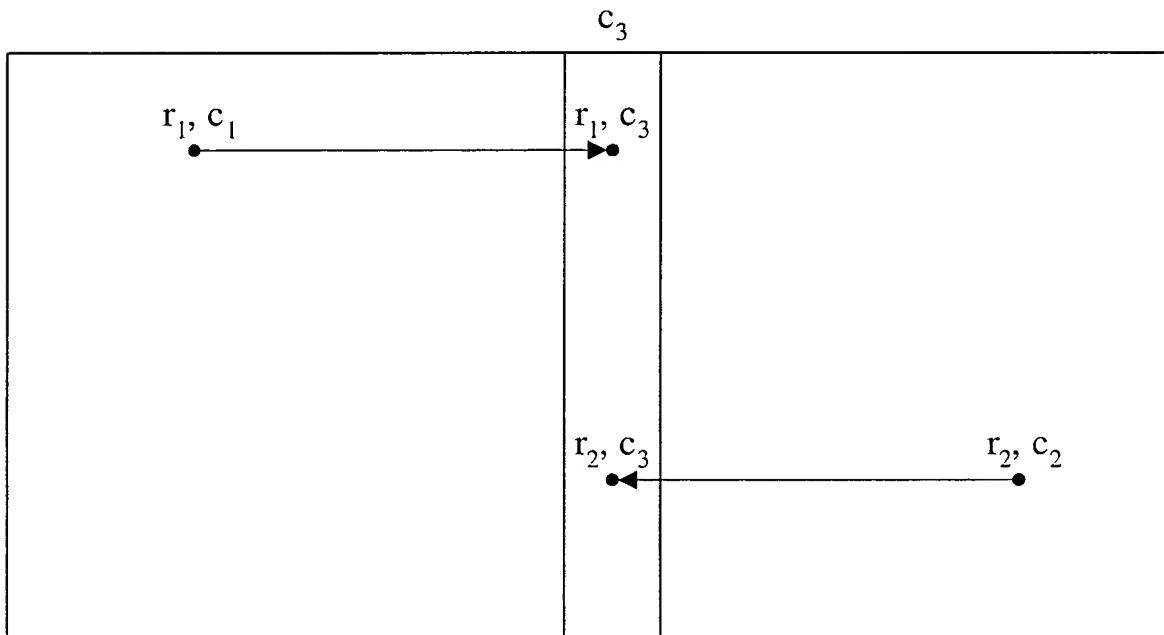


Fig. 6

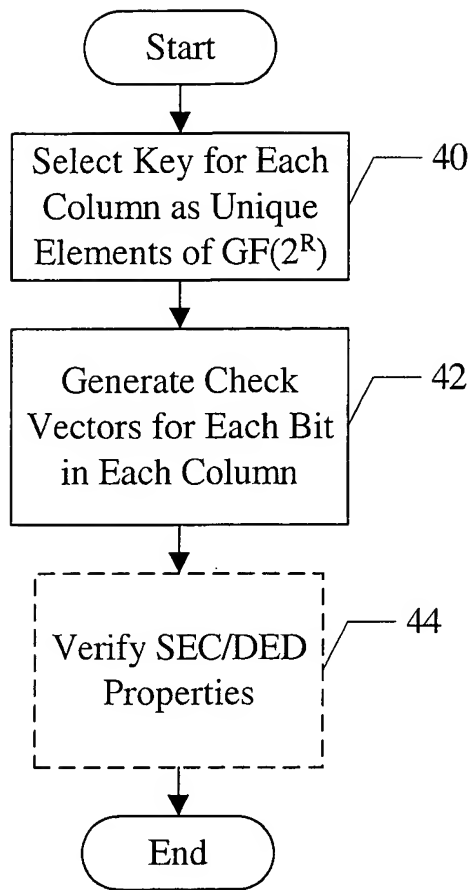


Fig. 7

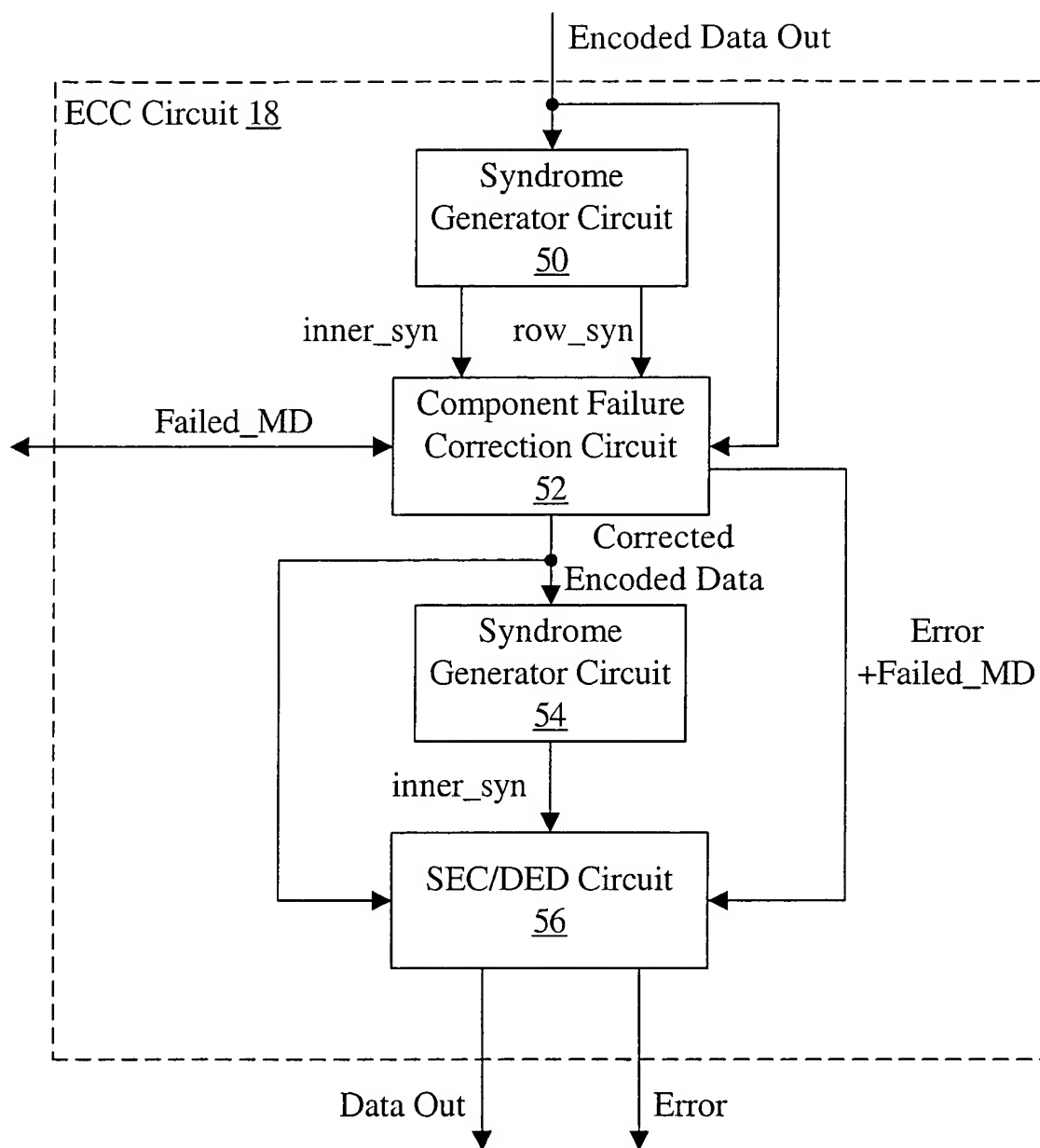


Fig. 8

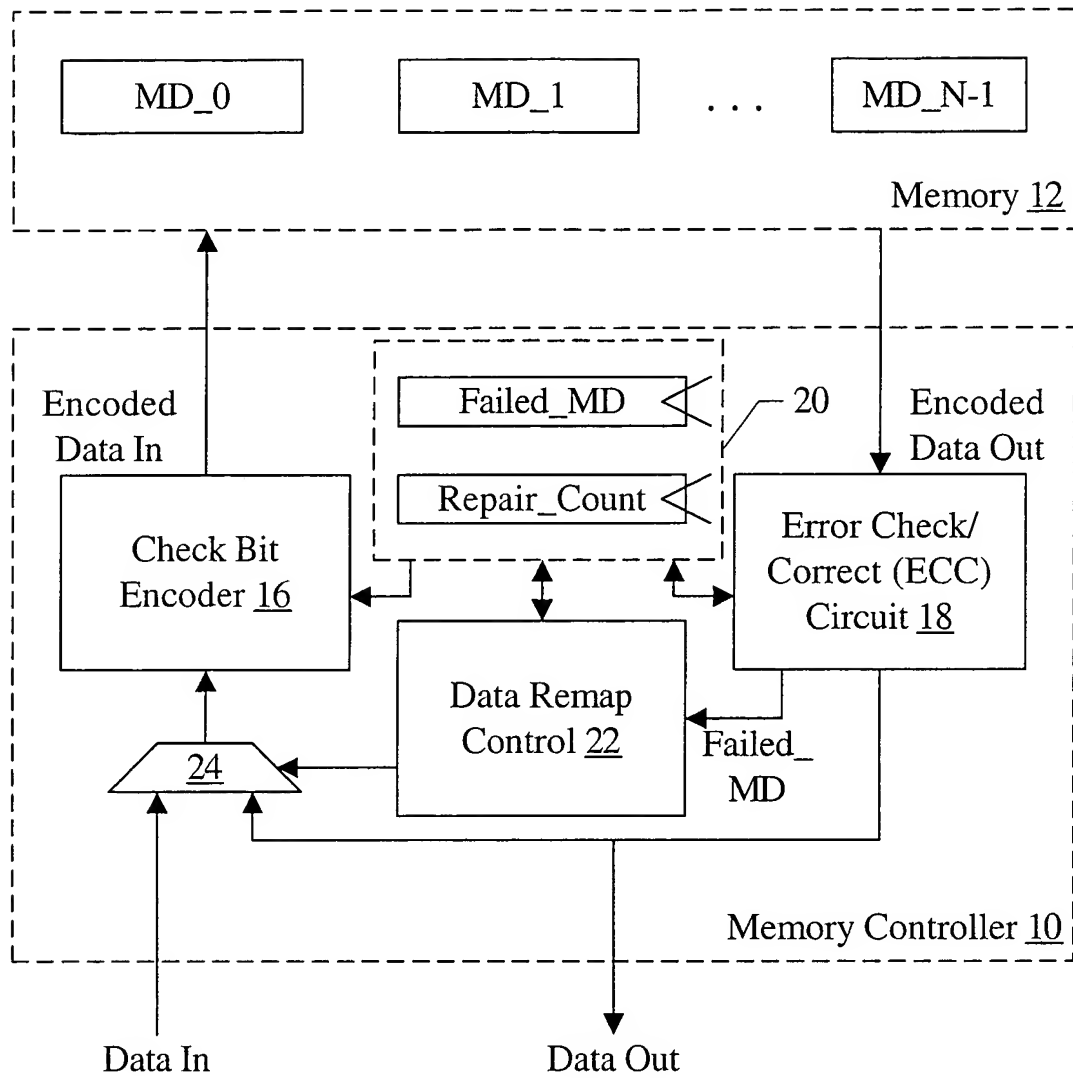


Fig. 9

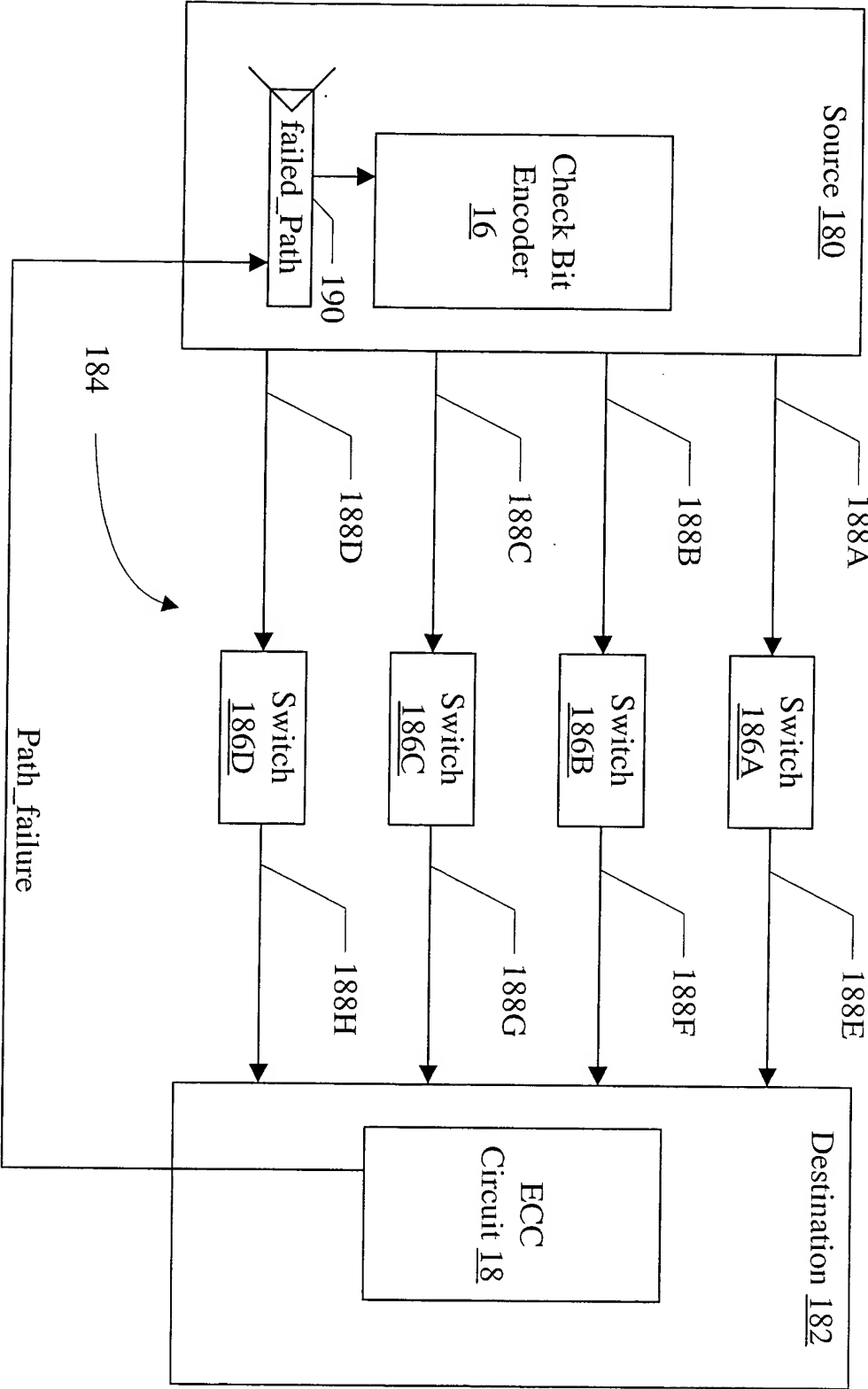


Fig. 10

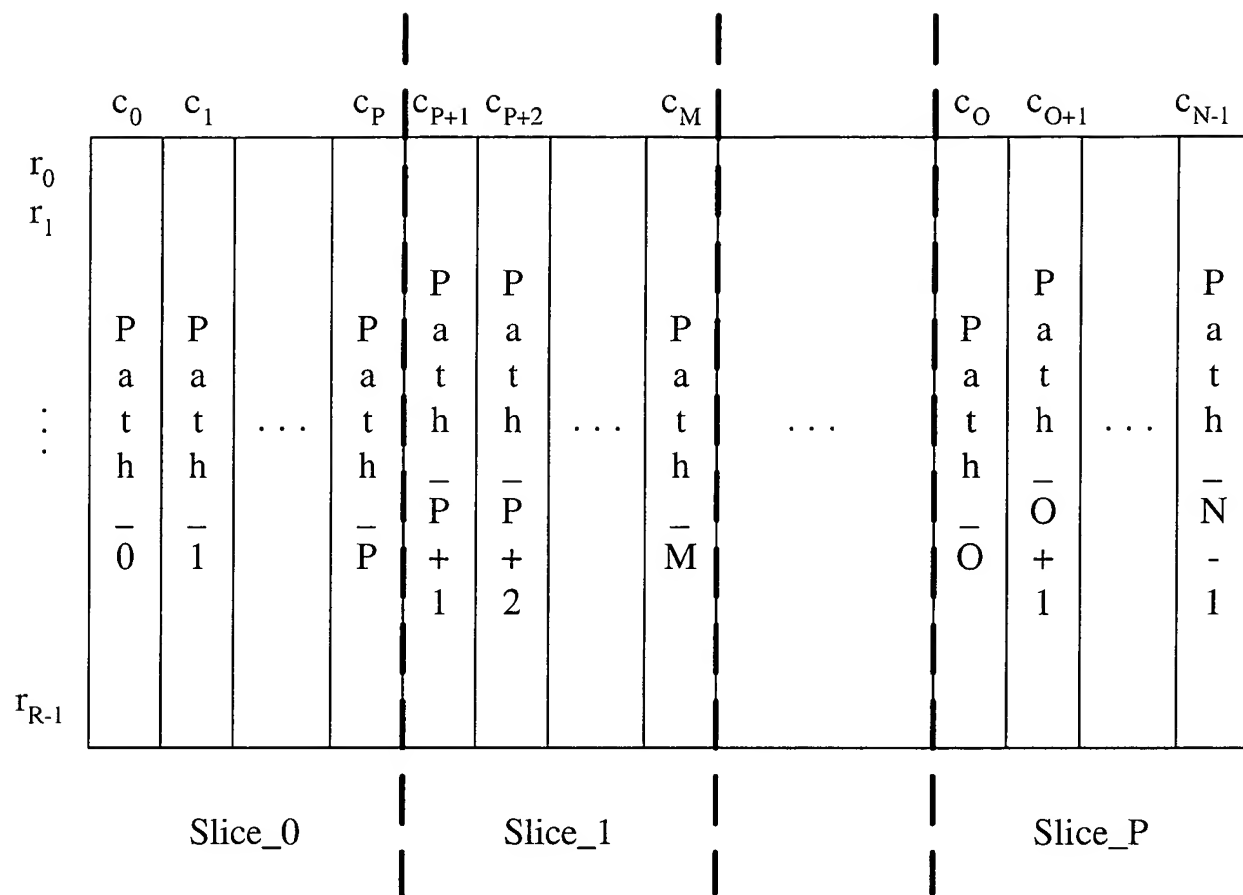


Fig. 11

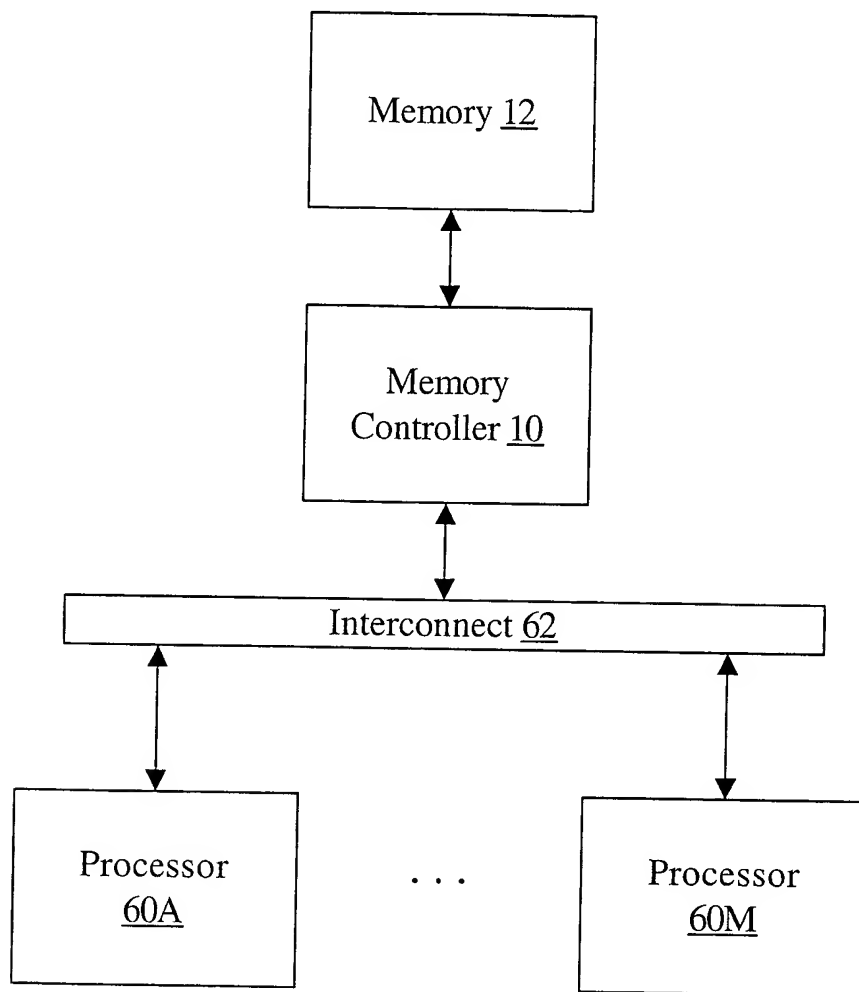


Fig. 12